Privacy and Security Tiger Team
Draft Transcript
May 4, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the Privacy and Security Tiger Team. This is a two-hour Federal Advisory Committee call, and there will be opportunity at the end of the call for the public to make comment. A reminder for workgroup members, please identify yourselves when speaking.

A quick roll call: Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Rebecca Rockland?

Rebecca Rockland
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Carl Dvorak?

Carl Dvorak – Epic Systems – EVP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
David McCallie? Neil Calman? David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Rachel Block? Christine Bechtel? John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel? Leslie Francis?

Leslie Francis – NCVHS – Co-Chair
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Joy Keeler? Sue McAndrew?

Sue McAndrew – HITSP – Deputy Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Vern Ranker?

Vern Ranker
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Deborah Lasky?

Deborah Lasky – ONC
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anyone off? Okay, with that I'll turn it over to Deven and Paul.

Deven McGraw – Center for Democracy & Technology – Director
Okay, terrific. Thank you very much, Judy. Thanks to members of the tiger team, staff from the Office of the National Coordinator, staff from the Office of Civil Rights who are with us in this call and of course, to the members of the public who join us. We always appreciate your input.

We have as always a full agenda today. I'm just going to give a high-level overview of what we're going to talk about today and then turn it over to Paul, my co-chair, for the initial couple of topics. We're going to talk a little bit about topics for future tiger team meetings. We began on our last tiger team call trying to flesh out some of the gap issues in terms of filling out a comprehensive privacy and security policy framework, and we've got those teed up. The folks from MITRE helped us, took some good notes and we are compiling a list. We also are soliciting some comments on the blog, and we're still taking those. So we're not trying to finalize those topics today but just to at least talk a bit about the list that we have to date, and then we're going to talk a bit about one of those issues, which is some follow-up items on certificate authorities who issue digital certificates.

Then, we are going to get started on a couple of topics that were definitely surfaced as gaps. They were actually issues that we placed on the back burner when we were doing our patient matching work, and that is issues of data integrity and quality and the patient's ability to request corrections. We'll spend a fair amount of time on the call going over some background information and then begin to talk about those issues to the extent that we have time on our call today.

Paul, I don't know if you want to add anything, but you're also next up to lead us on these topics.

Paul Egerman – Software Entrepreneur
Great. Well thanks, Deven, great summary. What we want to do is briefly review what we considered an initial list of topics for our future meetings. As Deven said, we have a commentary that's open on sort of like a rolling basis but we have asked for input by May 11th to inform of our summer schedule. This is on the ONC blog and so it's why I want to be clear that as I go through these topics, it's still sort of like a preliminary list. We want to get the public input and then hopefully with the public input plus the input from this meeting, we can try to put together a schedule as to what we're going to do. Deven said over the summer but I guess the summer includes the rest of May and June, sort of like a virtual summer.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Paul, I was late to the call. I just wanted to add my name to the list.

Paul Egerman – Software Entrepreneur

Great. Glad to have you David.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Sorry I'm late.

Paul Egerman – Software Entrepreneur
Here's the list of topics that we are perceiving right now. The first is actually as we discussed at our last meeting is to complete our policy framework for push transactions. So we've done a fair amount of that framework, but we want to complete that. That means addressing the issues of corrections that Deven mentioned. We'll be talking a little bit more about that in this call and then also other data integrity and quality issues that may or may not be there that we may decide that we want to talk about. So that's one topic.

The second topic is this whole concept of a query and response models for information exchange and since there are probably, I heard, they're definitely a whole series of privacy and security issues and challenges that are emerging from that, especially from the various information exchange models that are emerging. The third issue that we've identified is issues associated with hosted EHRs and basically there is an environmental stand being conducted by ONC. I personally do not know every … included in it in something called environmental scan but it sounds very impressive, so I'm sure it's a fair amount of work. So we're going to get that information in terms of existing security practices and various architectural models that I think is an interesting topic.

Fourth topic, very interesting, we mentioned patient portal issues beyond security and we have as an example transparency and usability. In the last few days or week, Carl Dvorak sent Deven and me an interesting e-mail where he made reference to the current controversies or discussions that going on around what happened with this Google—this Android phone and the iPhone tracking systems. A lot of people are very concerned about that, and it's sort of an interesting comparison. We want to make sure that there is transparency to patients that we don't have some similar situation where people are suddenly shocked to learn something about how their data is being stored or being used. This is a very interesting issue.

Number five is a HIPAA security gap analysis. Number six is very interesting issue that was also raised in our last meeting is internal unauthorized access. Some people think that that from a security standpoint is like really should be the number one issue we should be looking at as opposed to the external issues. But we've listed that topic.

Let me pause a minute and see what peoples' reactions are to this list of topics.

Neil Calman – Institute for Family Health – President & Cofounder
Paul, just to let you know, this is Neil and I joined.

Paul Egerman – Software Entrepreneur
Great Neil. Happy to have you.

Alice Brown – National Partnership for Women & Families – Director HITP
I also joined late. Sorry.

Joy Keeler – MITRE Corporation – Health IT Program Manager
And Joy.

Paul Egerman – Software Entrepreneur
Any comment about these topics?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They sound too hard to me Paul.

M
That's … they pay us the big bucks.

Deven McGraw – Center for Democracy & Technology – Director
I know. Maybe we should redo the public blog and ask for the easy ones.

Paul Egerman – Software Entrepreneur
These are interesting issues.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, very.

Paul Egerman – Software Entrepreneur
These are interesting issues and we thought we did the most complicated and most interesting issues first. I'm not sure we did. I think as you dive deeper into it, they're very interesting. The transparency issue, making sure patients aren't surprised is important. All these are interesting issues.

Deven McGraw – Center for Democracy & Technology – Director
I think the other thing that occurs to me is that with each of the issues, we might think about, even if it's temporarily, expanding our expertise to invite people who could help us to resolve some of these questions. I think for a lot of these issues, we could have hearings, and we might choose to do that but we're not going to have the time or the resources to do that on every one of them. So one technique that occurs to me that we could use is to ask people to join us for discussions that are particularly relevant to their area of expertise to help us out, in addition to continuing to seek public comment through the blog and on our meetings, etc. because they are hard. I think they're all hard.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Deven, the question that we eventually always get around to we get into these hard subjects is the lever arm question or the what context does it matter question. Are these broadly framed with some thought about what difference it makes in asking, for example evaluating the Security Rule gap analysis for HIPAA, I mean that's an OCR function. Are they asking for our input?

Deven McGraw – Center for Democracy & Technology – Director
I'm trying to remember because I recall that this got put on there because there was some work product that was being done internally that help us in this regard. Deborah Lasky—or am I mixing this up with the environmental scan?

Deborah Lasky – ONC
No, no, you're right. This idea has sort of two points of genesis. One is from some work that the Governance Team is doing and trying to establish what the criteria will be for organizations to join what we're calling the NwHIN. But more importantly, when we did our stakeholder input for the security strategic plan, a number of stakeholders, both from within HHS and outside, identified a need for this kind of mapping.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think it all sounds really interesting and I'm glad to be asked to render an opinion about it. It's just unclear of what the context of whom are we being a FACA at that point?

Deven McGraw – Center for Democracy & Technology – Director
I guess—I mean, we can't change our role. It is what it is to the extent that this is part of what ONC is looking at to inform the work that it's doing on governance then it sits within the purview of what the Policy Committee and it's working groups are typically asked to do. So it's not necessarily telling the Office of Civil Rights, for example, what it needs to do to HIPAA. But instead looking at if in fact we're going to have a set of practices or policies on the security side that go above and beyond the HIPAA baseline for as a condition of trust and interoperability for being part of NwHIN and then that would be something that would be within ONC's purview.

Paul Egerman – Software Entrepreneur
Any other comments about these topics?

Leslie Francis – NCVHS – Co-Chair
Just that they're wonderful. That was lovely.

Paul Egerman – Software Entrepreneur
Thank you Leslie. Again, to remind everyone, this is our tentative list. We're going to be waiting until May 11th to see what other comments come up on the blog. So if members of the public are listening, you can make comments at the end of this call but you can also make comments on the ONC blog. Then, what we are going to do is we are going to take this list of topics and we are going to do our best to establish a schedule that will take us through the summer months. So the intention would be to address all these topics, potentially by say the end of August. So that will keep us busy.

Deven McGraw – Center for Democracy & Technology – Director
Yes. It already sounds ambitious but I like your thinking.

Paul Egerman – Software Entrepreneur
Well we can do it. In America, all things are possible. The other thing that Deven mentioned is the certificate authorities and that's sort of like a piece of unfinished business that we have to address. To sort of refresh everybody's memory, there's a description of this situation on this slide. We did work on certificates—we're talking really about certificates at an entity level—and we made a number of recommendations. We handed it to the Standards Committee. The Standards Committee did a lot of work and then handed one issue right back to us.

They basically are asking us for some guidance on an issue of, in effect, what's the policy. What are the rules to determine who can be a certificate authority? Who can issue certificates for entities? So they're asking for policy guidance around CAs. Who issues them for—and again this is all oriented towards NwHIN, which I understand is now pronounced new-HIN. So, it involves defining a mechanism for establishing the legitimacy and trustworthiness of a certificate authority at the minimum level. Then you see on your screen, it talks about WebTrust, ETSI, it asks the question does the certificate authority need to meet the minimum standards defined for a trusted relationship with the Federal Bridge. We made a previous recommendation that we said the CAs should be accredited by ONC. I guess the Standards say we need to go a step further.

So you may look at this and say well you don't really quite know what all these different things mean and what we are proposing the way we would address this issue is to develop like a small task force to address these questions rather than having the entire tiger team do it, and maybe in that process possibly bring in one or two people who might have some specific experience with this issue related to certificate authorities and ONC through—is to provide support through Deborah Lasky, and we want to have recommendations be brought back to this tiger team by June 3rd. The reason for that is, is that that way we could make sure the tiger team understands those recommendations and then we bring it in front of the Policy Committee meeting, which is going to be done on HIT Policy Committee on June 8th, so we're trying to be responsive to Standards Committee. Standards Committee, I understand … has very much of a full plate and we'd like to wrap up this issue.

First, let me pause and see if my description of this makes any sense. Dixie, did I describe this correctly?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The only thing that I would clarify is you said this was around the NwHIN. The issue that we really want to address is not—the NwHIN already requires that certificates be obtained from certificate authorities that are cross-certified with the Federal Bridge. That's really not the issue. It's really the Direct exchanges, the exchanges using the Direct SNTP's protocols, e-mail protocol. In the case of those Direct exchanges, they really don't have any minimum requirements for where they get their certificates. So that's really the

focus of it. It'd be nice if everybody had it from someone cross-certified with the Federal Bridge but that's not the case.

Deven McGraw – Center for Democracy & Technology – Director
And when you say that, Dixie—I just have a question. Since we don't actually have the governance policies for NwHIN yet, are you talking about what we used to call NHIN Exchange?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. You're right. You're right.

Deven McGraw – Center for Democracy & Technology – Director
… of the DURSA because of the exchange of data with federal partners, the DA and SSA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, you're exactly right. When we use the term NwHIN, you're really talking about both NHIN Exchange as well as Direct?

Deven McGraw – Center for Democracy & Technology – Director
I think so. Essentially, I think when we use the term NwHIN, we're talking about the set of standards and services that they're developing through the governance rule that we don't know the exact scope of that yet. But I think it's fine to focus on NHIN Direct because that's probably where the question came from, but maybe to think broader about what that would look like for an expanded universe of exchangers in terms of certificate authority requirements.

Paul Egerman – Software Entrepreneur
Yes, I would agree. The scope ought to be for NwHIN and we should view the Direct project as a subset of NwHIN or as a stepping stone to it or something like that. So, we're building towards this end result, this end product.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think this is very timely because as we speak there's a group of about ten players in the Direct space that are actually having this exact conversation, a group that was commissioned by David Kibbe, but they're all basically participants in the various Direct pilots and/or are companies that intend to become large scale HIST providers like SureScripts. We are trying to hash out exactly the answer to these questions. We gave ourselves a June 10th deadline so if the tiger team can finish by June 3rd, that would be a good—

Paul Egerman – Software Entrepreneur
Well, yes because ... finish by June 3rd, we could present by June 8th, the Policy Committee and then David Kibbe's group won't have anything to do on June 10th.

Deven McGraw – Center for Democracy & Technology – Director
Well maybe there are some synergies to be realized by—

Paul Egerman – Software Entrepreneur
Or they could use that as a foundation for their work on June 10th.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that the real world issues that emerge from people who are actually out doing this for a living today are pretty important input.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I would agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And of course, they can do whatever they want because it's just an open protocol but if they want the name NwHIN attached to it, they're going to have to line up with these policies, so I think rapid convergence is in everybody's interest.

Paul Egerman – Software Entrepreneur
David, we have a lot of flexibility in terms of how we structure this task force, so we've pulling some or all of those people into it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and I think that some of them for sure would be—

Paul Egerman – Software Entrepreneur
Rather than have two independent efforts, let's just get it together, let's coordinate the efforts, that's what we're supposed to be doing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No I think that would be great, and I'd be happy to help play some of the bridging role because I am on the other one as well.

Paul Egerman – Software Entrepreneur
Great comment David, because that was also my question is who on this call would like to volunteer to be on this task force?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think I just did.

Paul Egerman – Software Entrepreneur
I think I just heard Dixie. Is there anybody else?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, I just confirmed that David just volunteered. Yes. I'd be happy to.

Carl Dvorak – Epic Systems – EVP
I'd like to join that as well.

Paul Egerman – Software Entrepreneur
Okay, terrific. We need somebody to lead the effort. Are you able to lead this Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure. I think it'll be short term.

Paul Egerman – Software Entrepreneur
Yes and we want it done by June 3rd. Is it reasonable we could do this all like in maybe two meetings?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
At least David McCallie and I have had a lot of conversations around this topic already on the standards side. David, you know this other group better than I do, far better. What do you think?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's surprisingly difficult when you get ten smart people, all of whom have a very slightly different but valuable angle on the problem. It's more cumbersome and exhausting than you would expect. On the other hand, I don't know any way to avoid it. They are subtle issues here that are fairly far reaching if you don't get them right, all the way from the cost of obtaining a certificate for yourself, if you're say a solo practitioner or a two-man or three-man practitioner, all the way from that all the way up to the Federal Bridge question, which has incredible impact on the cost of becoming a HIST if it's made mandatory. In fact, it may not even be possible to become Federal Bridge according to some of the opinions we've

gotten because Federal Bridge can only certify people who have a direct relationship with the government, so it's very complicated and we'd love the input but it's not simple. It's not a two meeting call, I don't think.

Paul Egerman – Software Entrepreneur
Well can we get it done by June 3rd? Is this a realistic plan?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think so. We just have to. I mean, otherwise we'll talk about it forever.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Well this is true, as is true of all of our issues, quite frankly.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think the group that David mentioned sort of compels us to do it early. But on the other hand, when we made this recommendation to the Policy Committee, at the same time, we recommended that the ONC undertake a cost benefit analysis of actually creating a healthcare bridge that would be cross certified with the Federal Bridge so that these HISTs could get certificates that could exchange information with CMS and VA and SSA and military health, etc. That study would really answer the issues that David brings up, and in fact might resolve the whole problem entirely.

Paul Egerman – Software Entrepreneur
So, I hear what you're saying but what I'm confused by is, are you're saying that we should not be focused on June 3rd? We should do some study first, ask ONC to do something first?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I would do. That's what I would prefer. I know Deborah Lasky's on the phone. Deborah, could the ONC address that request that we sent to you in the near term?

Deborah Lasky – ONC
Dixie, you're ruining my vacation plans, but yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then I think we should get that question resolved first because that's important. Some people have told us that establishing a bride-like—... already has established their own bridge with the Federal Bridge CA. So other people have answered those questions, and if we could establish a similar healthcare bridge to the Federal Bridge, that would really be a much easier answer.

Joy Keeler – MITRE Corporation – Health IT Program Manager
Dixie, the scope of the bridge that you just mentioned, the bio face one, is really a lot narrower than what I think we would be proposing in the healthcare sector. I think it would be important to scope this study accurately. So what kind of entities would you include in this?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So if I can jump in because we've literally had this exact discussion in the last couple of days, and there's e-mail—

Joy Keeler – MITRE Corporation – Health IT Program Manager
Yes, let's cut to the chase then.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So that if you want to really boil it down simple, let's say if you are a provider using Direct to communicate PHI data to other providers using Direct. And you wish to communicate to a provider at the VA or you wish to submit data to a secure mailbox at CMS, perhaps your quality data, do you have to have a certificate signed by something that is federally bridged? That's the simple question. If the answer is yes,

that the VA won't accept the security of your message unless your certificate roots to a bridge certified authority then that has huge implications on the cost of implementing Direct across the country.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well but that's what we asked ONC to find out. We already know for example that Verizon will provide any healthcare provider, a digital certificate for free and we know that Verizon is cross certified with the Federal Bridge. The question is what would it cost to get a small practice, which isn't a single provider, and that's what we don't know. I don't think it would be that hard for ONC to find that out.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right, and then the second question that has come up is, we were told by someone and I don't know who and I don't know what authority they spoke from, that the Federal Bridge won't issue certificates through one of its proxies unless it's to do direct business with the government. So if you have a small group of providers out there who never communicate with the VA and never communicate with CMS and they don't want to go through the cost and hassle of Federal Bridge, what do you do about them? According to David Kibbe that could be a significant number of providers.

Joy Keeler – MITRE Corporation – Health IT Program Manager
Okay so as usual whenever we talk about security, we've gone from the big picture and dived into the weeds pretty deeply pretty quickly. So we started out with asking how do we decide what would—the general policy question about what criteria you would use to decide what certificate of authority would be trusted and have segued very quickly into specific requirements of Federal Bridge. So I think that we probably want the big policy question answered as well as maybe the more detailed questions you're posting. Do you need to answer these detailed questions that you're asking in order to answer the big policy issue?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Joy, you're absolutely right. We got way down in the dirt pretty quickly there. But all I was saying was before we spend a lot of time figuring out what should be the minimum requirements for CAs, it would be nice to have back from ONC the feasibility of even having a Federal Bridge CA because if you had that, that whole other question becomes way easier.

Joy Keeler – MITRE Corporation – Health IT Program Manager
I think what you're saying is that cost is one of the factors that you would need to know. Is that it?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's exactly right, and we hear continuously, "Oh, the cost is enormous," and then in the very same conversation, we hear somebody say, "No it isn't." So we don't know, but I think ONC has the clout to find out pretty darn quickly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Joy, I apologize for getting into the weeds but those of us who are building and deploying systems that can use Direct are at that level right now trying to answer these questions.

Deven McGraw – Center for Democracy & Technology – Director
I get that, but keep in mind David, that the policy recommendations of the tiger team are going to get surfaced to the Policy Committee to decide. So we have to actually stay at a level that will enable adoption by the Policy Committee, but further specification of details doesn't necessarily have to be done by our body, the tiger team, or the Policy Committee.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right but to answer the detailed question, one needs a policy statement. I'm happy to mask the detail question but the policy statement that emerges will answer that detail question. So we need to make sure we understand what policy questions are important because they're the ones that will affect what people are going to go and do, and they will frankly determine whether Direct succeeds or fails.

Joy Keeler – MITRE Corporation – Health IT Program Manager
I think that this could be a vipercated process, part of which belongs with the Policy Committee and part of it which I think is more of an offline conversation with this group that you're talking about that's raising these issues with ONC directly to find out if we could provide that sort of research to inform that specific issue. Then that answer may help inform actually who would meet these criteria, but I'm imagining what you said is how do you decide what qualifies for certificate authority. The broad policy answer might be something which isn't hideously expensive or something a little bit more diplomatically than that. So that's your policy and then what you're asking us for is how expensive is this stuff really, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Is it in fact policy that you can't communicate with the VA unless certificates that asserts your identity have been issued by a bridge authorized partner. Is that a true statement or not is question number one. Then question number two, if it's true, how expensive is it?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I have maybe a question that's off topic, but are there other costs associated with VA related transactions or doing this? What I mean by that is, like the VA when we do business with them wants us to comply with FISMA. Are there other types of requirements that might be ancillary to actually getting a certificate from a bridge authority like that or is this an entirely separate matter?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think they're related. So for example, if you want to become a Federal Bridge certified certificate authority, you go through FISMA audits.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But what about people that would get certificates from those bridge authorities and want to transact with the VA, would they also need to have to comply with things like FISMA or is that going to be a—?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No. I think they would be issued a certificate at a certain level of assurance and the rigor of the assurance would vary based on the level of assurance but it would not be at FISMA level.

Paul Egerman – Software Entrepreneur
Let me interrupt though because we are getting into the weeds. This is starting to get fairly technical. I like the way that I thought I heard Joy sort of describe this that there's sort of like two aspects to it. There's a policy aspect discussion and there's actually a much more detailed, technical aspect. So on a policy basis, one could say something like, well you have to have a certificate authority and that certificates have to be at a reasonable enough cost so that small group practices can afford it. Then you could say if you wanted to—and the certificates have to be valid for dealing with the Veteran's Administration, with VA, or dealing with NHIN Exchange. So you could say well you say that's a policy then we try to figure out how in the world we can implement that policy. Is it doable? Or you could also have a policy that says, well we're going to have two certificates. You get the certificate for NwHIN but if you want to deal with the VA, you have to have a second certificate. That might be another policy that you could have, so I think there is a policy discussion, and I think we could get started with that and through the policy discussion, you could raise whatever questions you want ONC to specifically answer.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think the policy question, especially with CMS, the one that David brought up, is would they expect a certificate from any certificate authority or does it have to be federal? I think that this is a very opportune time for ONC to have that discussion with CMS because as I understand it, up to this point, CMS hasn't accepted electronic submissions. So I think it's a perfect time to have that policy discussion with them.

Paul Egerman – Software Entrepreneur
So what I'm suggesting is we could reformulate this by saying, here's the design we would like. We would like these ... to be able to get one certificate from a certificate authority and we would like it to be all-purpose. It would work with CMS, it would work with NHIN Exchange, it would work with NwHIN, and

it's got to be reasonable cost. As a result, here are the questions we need to get answered or possibly here are the changes that need to occur. Am I getting this right or wrong, Joy? Would that be a helpful way to go about this?

Joy Keeler – MITRE Corporation – Health IT Program Manager
Yes. I think so. What I would like is—because I find it hard to take good notes while I'm listening to this, is if David could send me the questions that he would like answered offline and cc Deborah and everybody else who might want to be cc'd with that so that we're sure that we're answering the right questions.

Paul Egerman – Software Entrepreneur
So, what we need to do is we need to make sure, right, that we have a direction. The direction is to try to write this policy statement that isn't necessarily burdened with knowing how things really work right now but really write it the way we would like it to work. Find out what are the questions that need to be answered to get to the place where we would like it to work and see if we can get that theory and reality to get together. So that would be one thing.

The other thing that is seems we need to do is to get together with this other group of ten people that David Kibbe is doing and see if we can coordinate our activities. It's crazy to have three different groups trying to attack the same issue.

Joy Keeler – MITRE Corporation – Health IT Program Manager
Well it depends on who the groups are, Paul, and what the composition is.

Paul Egerman – Software Entrepreneur
That's right. So, is there enough here to suggest that we at least get initial meeting going? That Carl, David McCallie, Dixie, and Deborah Lasky and maybe we bring in a few other people from this other group, we have an initial discussion and have a meeting … initial discussion and try to see if we can get this whole process launched?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That sounds good to me Paul.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That sounds good to me. I would suggest to the ONC team that if it makes sense for you guys to include Arien, you might wish to ask him to participate as well.

Paul Egerman – Software Entrepreneur
David that's a great idea. Let's see if we can add Arien to the team and you might have some suggestion as to how to coordinate this process.

W
See this is what happens when you're not on the phone call.

Deven McGraw – Center for Democracy & Technology – Director
Who else isn't here? We'll sign them up too.

Paul Egerman – Software Entrepreneur
Let's make sure that they do all the work. Arien's great and I think this can work. So Dixie—and we'll make if you don't mind David, since you seem to be volunteering, we'll make you like a co-chair of this task force. It's sort of like a field level promotion here, battlefield promotion, and let's go ahead and launch this. I still would like to stick with the June 3rd target if that's acceptable to you unless you tell me after you eat lunch there's no way you can do it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think we can do that. I think they're just some fairly straight up decisions to make. They're complicated but they've just got to get made.

Deven McGraw – Center for Democracy & Technology – Director
Sometimes it helps to set yourself a deadline.

Paul Egerman – Software Entrepreneur
Are you comfortable with all this, Carl?

Carl Dvorak – Epic Systems – EVP
Yes, it's good time.

Paul Egerman – Software Entrepreneur
Okay so that's the certificate authority. When you set it up, let me also try to participate in the meeting to see if I can be helpful too. Dixie and David, I'm not going to abandon you. We're going to get this thing done.

Deven McGraw – Center for Democracy & Technology – Director
I will try as well. We don't want to abandon you but we really needed some help, some people to focus on this intensively, so that we could be working on some things really simultaneously, which is something we talked about doing many times. This may be the first successful endeavor at actually getting it done.

Paul Egerman – Software Entrepreneur
So, that's the issue of the certificate authority. So I went through the topics, I went through certificate authorities and next what's going to happen is Deven's going to take us a little bit through some of these issues about data integrity and quality and corrections.

Deven McGraw – Center for Democracy & Technology – Director
Thank you Paul. Nice job. Alright, so as we have been doing throughout our history as a tiger team, which I think we're pretty quickly coming up on a year together, we have taken the principles that ONC has adopted in the nationwide privacy and security framework for electronic exchange of individually identifiable health information—abbreviated here because it's a really long term to spell out as IIHI—and tried to flesh that out with policy recommendations. When we took that framework document, which is what is posted on the blog and what we have tried to update with each set of recommendations, there was a glaring gap with respect to how to flesh out the principle of correction. We knew that because this set of issues actually did come up, and we talked about them a bit but did not resolve them in our patient matching discussions. Then the other issue is the other principle that has some gaps in it and is related to this because it does in some ways have to do with data accuracy and correction and that is data integrity and quality.

Before we begin to talk about what might be a set of policy recommendations that we would put forward for each one of these categories, I thought that it would be helpful for us to understand a little bit more about what's in these principles. What's in each of the principles; what we've already got in terms of some standards or rules whether in certification standards or whether with respect to the HIPAA privacy or security rules. So we prepared some background slides here, but I'm fully acknowledging that as I'm going through this, that there's a lot of expertise on the phone, in particular folks here from the Office of Civil Rights. We've got folks here from the Standards Committee on the certification standards. We've got ONC staff, and so even though there's a lot to get through here, I do want to pause and make sure that number one, this information that I'm conveying is correct and of course to allow people to ask questions. Then what we have after we lay out the background and get everyone on the same page is a set of draft questions that we hope would stimulate discussion. Paul will take back the lead on the conversation in that part and see if we can't start to flesh out some of the policy parameters that we would need to fully explore in our next call.

With that, we'll start with what is the ONC principle of correction. It is claimed as an individual right, which is that individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or have a dispute documented if their requests are denied. That's the principle in short and then there's actually a little more text, some more detail about it that's in the Nationwide Privacy and Security Framework. It's on the Website. It was issued in 2008, and it just sort of fleshes this out in a little bit more detail.

I won't read this in its entirety but it acknowledges the important stake that individuals have in the accuracy of their data and the consequences that can occur when data is not accurate and yet is communicated downstream. Therefore, it's essential for individuals to have practical, efficient and timely means to dispute accuracy and to have it either corrected or a dispute documented and to have the correction or dispute communicated to others with whom the underlying information has been shared. Then it goes on to say that persons and entities that participate in a network for the purpose of electronic exchange of IIHI should make processes available to empower individuals to exercise a role in managing their identifiable health information and should correct information or document disputes in a timely fashion. So that's the correction principle.

There's a separate principle on data integrity and quality. This applies really at the provider level. Persons and entities should take reasonable steps to ensure that individually identifiable health information—I didn't use the acronym here, but IIHI—is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner. So that's the short version.

Then of course, they added some more detail in the text, again acknowledging that completeness and accuracy of health information has an impact on healthcare quality and outcomes. It also again, talks about how persons and entities that participate in a network for the exchange of identifiable information have a responsibility to maintain identifiable information that is useful for its intended purposes, and this involves taking reasonable steps to ensure the information is accurate, complete and up-to-date and has not been altered or destroyed in an unauthorized manner. Persons and entities have a responsibility to update or correct individually identifiable health information and provide timely notice of these changes to others with whom the underlying information has been shared. Moreover, persons and entities should develop processes to detect, prevent and mitigate any unauthorized changes to or deletions of identifiable health information. So that's what's already been expressed in the Nationwide Privacy and Security framework that ONC issued back in 2008 and then is part of the strategic plan.

So other relevant provisions that I think we need to know about are that there is at least one that I could identify—and I'm counting on tiger team members and others to let me know if there's any that I've missed, but there's at least one certification provision that's relevant to these two principles. That is the integrity provisions for EHRs that require demonstration of the capability to create a message digest in accordance with the hashing algorithm standard and then the ability to use that standard in order to verify that the message has not been altered in transit. Then, also the ability to be able to detect an alteration of audit logs.

I just want to pause there and see if I've missed any provisions in EHR certification that are relevant to either correction or data quality and integrity that I should have included in these background slides.

Leslie Francis – NCVHS – Co-Chair
Deven, one thing I would like to emphasize is that the really important difference between correcting your own record and the issue of communicating to others when a correction has been made. That adds a whole new dimension that HIPAA didn't think about.

Deven McGraw – Center for Democracy & Technology – Director
Well we're going to actually talk about HIPAA, what HIPAA does and doesn't do in just a second. So—

Leslie Francis – NCVHS – Co-Chair
But that's not just the fleshing out of correcting your own record—

Deven McGraw – Center for Democracy & Technology – Director

No you're right.

Leslie Francis – NCVHS – Co-Chair
I think it's critically important but it's just different.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I mean there's actually a theme here that there is a difference between the principle of corrections and how HIPAA treats that issue, which is focusing more on a patient's right to make a request for a correction. Versus a principle of data quality and integrity, which talks about what are the provider and institutional obligations with respect to data accuracy and communicating that forward. So this is a little bit different.

Moving on to the HIPAA provisions, the Security Rule provisions that I was able to find, largely address the issue of integrity not as much specifically to data quality with integrity really just being defined as the property, the data or information has not been altered or destroyed in an unauthorized manner. There are provisions in the Security Rule that require covered entities to assess risks to data integrity and implement measures to reduce these risks to reasonable levels. Covered entities also in a separate provision need to implement policies, procedures and controls to protect electronic protected health information from improper alteration and destruction. So in terms of the certification provisions of EHRs and the Security Rule provisions that we've highlighted here, there's a focus on the integrity aspect, the ability to protect data from being altered or modified or destroyed in a way that's not authorized.

Then, the Privacy Rule actually has some fairly detailed provisions on individual's right to request a correction to data that's in an electronic medical record that's about them. Now, I didn't find any HIPAA provisions that deal with covered entities. For example, obligation to correct data and errors that say the covered entity might unearth on its own, not necessarily prompted by a request from an individual. Certainly if I've missed something, I hope that folks will chime in, but it's my understanding that the Privacy Rule has focused on what happens when an individual asks for a data correction. It's very clear that individuals have the right to ask a covered entity to amend protected health information and this is whether it's in electronic or paper form in what's called a designated record set, which is a HIPAA term of art but it does cover both demographic and clinical information that's in an EHR.

A covered entity actually may deny the request if that entity didn't create the information, unless the originator of the information is not available to act on the request. So it means that patients aren't necessarily required to go to the source in order to get a correction but if they go to a downstream entity, that entity wouldn't have to make the correction unless the originator or the original source is not available. Covered entity may also deny the request if it's the type of protected health information that the patient doesn't have a right to access, and there are categories of information to which that applies, or if the entity believes that that information is in fact accurate and complete. In other words, the entity actually thinks the record is accurate and the patient is not correct.

So getting through these slides—and again, I apologize for the volume of material but I think it's important for us to understand the scope of what's out there before we dive into what additional policies, if any, may be needed. A covered entity can require a request for amendment to be in writing and that individuals provide a reason. They've got 60 days to act on the request although this can be extended for an additional 30 days if they need to and they specify the reason and the date for completion.

If a covered entity agrees to the amendment—and we have of course provisions for it they disagree, but if they agree that they're going to amend the information at the individual's request, at a minimum, they have to identify the records that are affected. And either append or otherwise provide a link to the location of the amendment to inform the individual that the amendment has been accepted and get the individual to identify and then agree to have the covered entity notify relevant entities that should receive the amendment. Then they have to make reasonable efforts to inform and provide the amendment within a reasonable time to the persons who have been identified by the individual as needing to receive it. But also persons including business associates that the entity knows has the PHI that has to be amended and that may have relied or could foreseeably rely on the information to the detriment of the individual.

Now if the covered entity denies the amendment, they have to provide the individual with a written denial that includes the basis for the denial and information about the individual's right to submit a written statement of disagreement. The individual chooses not to submit that statement of disagreement, they can request that the covered entity provide the request for amendment and the denial with any future disclosures of the disputed protected health information. The covered entity has to let the individual know that they have the right to have this information conveyed with any future disclosures, but they only have to convey that information with future disclosures if in fact the individual asks for that action to be taken.

Then if the individual actually does submit the written statement of disagreement, then the entity may prepare a rebuttal. It's like a mini-case going on with this data at this point, a copy of which must go to the individual. Then, with respect to that protected health information that's in dispute, the covered entity has to append or link the individual's request for the amendment, the denial that came from the covered entity, the individual's statement of disagreement, if they've in fact provided one, and the entity's rebuttal, if the entity has done one, to the information. Then include it in any future disclosures and if that's a pretty lengthy amount of documentation, the covered entity has the option of instead providing an accurate summary of this information that is appended to the disputed data. Then, the final provision is that if you are a HIPAA covered entity and you receive notice from another covered entity that it has granted an individual's request for an amendment of data, you have to make that change to the information in your records as well.

I want to stop there, mostly because we're done with that long explanation, but I also want to pause for a moment and ask if the team from the Office of Civil Rights wants to correct anything I said, if I got it wrong or to add any information that I might have missed. It's important for us to understand how HIPAA covers this important issue.

Sue McAndrew – HITSP – Deputy Director

Good job. I don't think we have anything necessarily to correct. I will just say that one of the things that we struggled with and attempted not to try to control through the privacy rule were the practices and policies that were in place with regard to laws governing the maintenance of the medical records. So we get the question a lot, "Well, why can't you just erase something and put in the correct data?" A lot of the appending or linking to was done in order to allow entities to preserve the fact that they may not be allowed by law to just do what we normally think of as a correction to the record.

Deven McGraw – Center for Democracy & Technology – Director

Right, those laws are those laws are largely at the state level, right?

Sue McAndrew – HITSP – Deputy Director

Right. So we weren't writing on a blank slate. We did not want to ... authorities for what had to be in the medical record and when authorizing people to take information out of the medical record. That wasn't our purview.

Deven McGraw – Center for Democracy & Technology – Director

Does anybody else have any questions about any of the background material that we've presented before we start moving into potentially scoping out the questions that we might want to answer?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I have a question. This back and forth described here as you called it a mini-case of argument and rebuttal and counter argument is it required that humans be involved in the process of disseminating a correction? Or is it conceivable that a system, which propagates the corrected, amended version automatically to say downstream dependents and properly updates the downstream dependent of the correction could happen without human intervention? Is there some implication here that human acknowledgement is required at every step along the way or could this conceivably be done automatically?

Sue McAndrew – HITSP – Deputy Director

I think the mini-case arises when the entity is denying the correction. So if you're denying the correction there's nothing to propagate downstream.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
In which case humans have to be involved clearly.

Sue McAndrew – HITSP – Deputy Director
So all of this is just to ensure that the individual has a right to make their position known with respect to data in their records if they feel it's inaccurate and then to fully air the covered entities side of the case as well. So that people using the information downstream who may get it from the entity later on, are put on notice as to the nature of the dispute and they don't look at this information—well they may look at the information in slightly differently.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have a question. It's hard to keep up Deven, so I'm kind of looking at the slides as well.

Deven McGraw – Center for Democracy & Technology – Director
Oh, that's okay and if you want me to go back to a slide I can, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
On slide 17, it says that the covered entity data recipient that receives notice from a covered entity that it granted an individual's request, but there's really no requirement that I see in these slides, there's no requirement that an entity actually send such notice. Is that right?

Deven McGraw – Center for Democracy & Technology – Director
Wait so actually if they have agreed to the amendment—and I'm going back to slide 15—they actually do have an effort, they have to make reasonable effort to inform and provide the amendment to anybody that the individual has identified as needing it. And persons including business associates that the entity knows have the PHI that needs to be amended and that may rely on it or could foreseeably be relying on it to the detriment of the individual. I guess it's a judgment exercise that they make, but it is an affirmative obligation to push it downstream to again people identified by the individual who has asked for it and potential downstream entities that might rely on it to the individual's detriment.

Leslie Francis – NCVHS – Co-Chair
Deven, that is weaker than the other principle because essentially the idea of that is if you know because you've transferred the record, then you have a responsibility to transfer the correction. But that's really different from the idea that if a record is going out through an exchange and it may have been exchanged and then re-exchanged, that a really good idea would be a way to be able to follow a change across exchanges.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's not in the law as it's written today, right?

Deven McGraw – Center for Democracy & Technology – Director
Not the law but you're saying, Leslie, that the language of the principle of corrections that is in the ONC data sharing framework that we went over in an earlier slide seems to be stronger.

Leslie Francis – NCVHS – Co-Chair
Right. One of the things that could very easily happen if you work with the HIPAA framework is that within the ... of where the covered entity has sent the record, that's where they know it's gone or where the patient knows it's gone, the correction goes. But that's not the same thing as attempting to figure out or having even technological ways to figure out every transfer that's occurred with that record or every download that's occurred with that record so that the correction can follow the record. You see what I'm saying?

Deven McGraw – Center for Democracy & Technology – Director

Right. Well I do but it’s almost if one could read the HIPAA provision as saying, well if it’s a correction to demographic data where it’s street and not road, that’s one thing. If it’s a correction to what’s the medication that I’m on, that might be different. They made a judgment call about what types of changes should be affirmatively pushed forward and which ones just don’t necessarily need to be.

Leslie Francis – NCVHS – Co-Chair
But HIPAA works on whether the patient has asked … what are the covered entity reasonably should expect, and that’s different from trying to figure out a technological way with massive potential for exchanges of information to downstream push corrections to follow the record. I don’t know if that’s possible technologically.

Deven McGraw – Center for Democracy & Technology – Director
I think that’s right but before we launch—we’re starting to sort of launch into a discussion of sort of the merits of what a set of recommendations might look like. That’s good, but before we do that, I want to make sure that there isn’t anybody else on the phone who had a question about some of the law that we just went through.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
If I could just drill in on Leslie’s question and maybe ask it more directly. Does HIPAA imply any obligation to propagate a correction if the patient has not expressed an interest in it or is it only triggered if the patient expressed an interest?

Deven McGraw – Center for Democracy & Technology – Director
The latter and Sue and Vern please correct me if I’m wrong, but it’s triggered only by a patient request.

Sue McAndrew – HITSP – Deputy Director
The mandate and the rule are only triggered by—they start with the individual’s request to amend. We didn’t think that we needed to speak to the entity’s own interest in data integrity. So we did not regulate that as a matter. We don’t prohibit it.

Paul Egerman – Software Entrepreneur
You also probably did not contemplate wide spread information exchange because that really hasn’t existed so far.

Sue McAndrew – HITSP – Deputy Director
Well clearly we were scaling the requirements to a paper world and small doctor practice, and were not envisioning as Leslie was hypothesizing an information tracking system that could contain strings of history of where data originated and every place it’s been.

Paul Egerman – Software Entrepreneur
So when you did these regulations, the image I have—and tell me if I’ve got this right—is you’re picturing like a physician’s office with a paper record that maybe the patient transfers to another physician so the record is now copies made and given to another physician’s office. Then somehow the patient comes back to the original physician and complains about something in the record. You’re saying well in that case, it was the original physician’s got to fix the record and they’ve got to also send it downstream to whoever was the other physician. You almost think about it in terms of paper documents.

Sue McAndrew – HITSP – Deputy Director
Yes. We were clearly thinking not exclusively but predominantly that it had to be scaled to work in a paper environment where, as Deven had mentioned, we drew the threshold where the information if it did not get amended would be actually harmful to the individual as opposed to changes just for the sake of a totally pure record. Then entities—and then trusting on HIPAA as a floor to certainly show a path at least that they wanted to go above and beyond what they could do.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Any other questions before I turn it over to Paul, which since we already seem to be chomping at the bit a little bit to start talking bit about what sort of questions we might want to address from a policy standpoint with each of these principles. Again, corrections really focusing on, even at the ONC principle level, what's the individual's right to ask for data to be corrected or to have a dispute appended? Then with respect to data quality integrity, what are institutional obligations on data accuracy and informing downstream providers of errors that they may discover? So, Paul, you want to take it away?

Paul Egerman – Software Entrepreneur
Sure and before I go through the questions actually I was going to ask questions of the members of the tiger team, my impression—I was trying to talk a little bit, not about what's the laws and regulations say but rather very briefly how these EHR systems are currently implemented. My impression is that there's a fair number of corrections that occur based on providers seeing things and changing things after the fact of data quality issues and late arriving information and so on and just plain errors. There's very little that occurs in terms of patient corrections mainly because patients don't have a lot of access to this material. Is that right or is that not right? Is that changing?

Carl Dvorak – Epic Systems – EVP
Paul, we've got somewhere between eight and nine million MyChart users that do occasionally have a correction request. There's typically, it depends on the site, but some sites will configure a message in the messaging subsystem of the portal to go to medical records when a patient feels something is not expressed properly in the medical record. Then just as Deven went through, it's a wide variety of things all the way from they don't like to have their condition portrayed that way but it's factually correct to uh oh a doctor picked the diagnosis code that was just wrong and needs to be corrected and changed.

So it happens. It's not common yet, but it does happen. When patients have portal access, if things are wrong they get it fixed quickly. If things are said in ways that they prefer they'd be said differently, those happen but there not treated—the organizations tend to not change the records for those kind of reasons very often.

Paul Egerman – Software Entrepreneur
Does it happen often that there's disputes?

Carl Dvorak – Epic Systems – EVP
Yes. Not again often. I hear of them occasionally so I shouldn't say often ... backdrop, I don't know. I hear them from time to time, drug-seeking behaviors in particular. Those kind of things will sometimes be put up as a problem on our problem list and patients might get visibility of that once in a while but—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Patient corrections are incredibly rare as an event. They just don't happen that often. When they do, many times they're very I hate to say this, sometimes the patient … misplaced in their reasoning behind asking for the correction.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Although there's some extremely well documented cases where the patient corrections avoided a wrong limb from being amputated.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
By the way, often the physician or other clinical staff will identify a mistake in the record and will make the change too, but as to Carl's point, often they're qualitative changes that the patient wants the record not—

Joy Keeler – MITRE Corporation – Health IT Program Manager
Carl, I have a question for you. I know in the paper world, just from when I was on the outside and was doing a lot of work on patient access rights, I would often receive calls from people who said, "I've got a copy of my medical record and it's got tons of information in it about a patient that is not me." Does that happen as much in the electronic world?

Carl Dvorak – Epic Systems – EVP
It does. Again, it's not common but you will occasionally have a clinician accidentally chart into the wrong chart electronically.

Joy Keeler – MITRE Corporation – Health IT Program Manager
What do you do when that happens?

Carl Dvorak – Epic Systems – EVP
There's a process. Again, it varies a little bit by site but generally, what they do is they move that information into the corrected chart and then they void it out in the current chart. They leave a little bit of a trace in there, in part because if someone else had made a decision based on that data being present even though it's erroneous, the decisions may have been made on it. So they tend to void it out, leave a trace of it and then pull it out of all the key list so they'll take allergies problems out, and they'll create a little entry in the chart that says this was once here. It is moved to the correct patient but for reference, you can still see it in there, but generally it's blocked from the patient view.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Often where this occurs is when somebody is committing identify theft. They're seeking medical treatment using someone else's identify and we have to untangle the record after the fact.

Paul Egerman – Software Entrepreneur
I have to tell you when I was doing eScription, we saw this happen a lot. Physicians would dictate on a patient and they would get interrupted or confused and they would start dictating on the next patient without realizing they hadn't finished the first one. So you would get a document that had information on more than one patient and sometimes it was noticed before the physician officially signed it into the record and sometimes it wasn't.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
In those cases, people are always very willing to make the change. That's typically not in dispute.

Paul Egerman – Software Entrepreneur
Sure, if the patient notice it, and frequently what would happen is it would get noticed again like a month or two or three later because the patient would come back and someone else would read the record for the first time and see that there was something that was just clearly incorrect. Those would frequently get handled would usually be an amendment, you would put in effect an amendment to the note that said, "The previous note is incorrect. Here is the correct information." So you would actually not do the process that Carl said. You'd leave the other thing there but you'd somehow indicate it as obsolete and say this is the corrected one.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But the more contentious issue is where a patient comes into the emergency department and they're drunk. The physician at the emergency department says, "The patient was inebriated when they presented themselves to the emergency department." The patient comes back after the fact and says, "No, I was not. I want that out of my record." The physician's saying, "Yes, you were." The patient says, "No, I wasn't." So those are the types of things that occur every once in a while, and they're the ones that are problematic.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Just to put another angle on it, back Paul to your original question, I think well-defined system interfaces that drive from a source out to dependent systems using an interface style push model will generally, at least the ones I'm aware of, will propagate the corrections correctly, the amendments. We use a lot of strikethroughs sometimes to preserve the original text so you can still read it but it's struck through. They will preserve that out to the dependent systems. The place where it gets more problematic is if you have something like an HIE where the consumer, the eventual consumer of the data doesn't have a directly connected interface. They may pull a copy down out of the HIE but that's now a broken link, if you would.

So the propagation won't automatically happen out that far. I think that'll be something that we end up getting into.

Paul Egerman – Software Entrepreneur
Well and that's a good segue David into what are the questions. So if you look at the screen, there's two questions here that we—and I'm going to take you through these two screens and then I'm going to pause. Rather than answer the questions, what I want to say is what are the right questions that we should be trying to ask ourselves to answer?

What I'm going to try to do is say here's what we thought were a good series of questions, ask for you to react to it and fix it and see what is the right questions that we should be asking about this whole corrections process so that you see two on the screen. I'm actually going to do the bottom one first. The first one really says do certified EHRs have the correct capabilities to comply with the HIPAA rules regarding corrections to the EHR, which is there functionality for appending or amending information into the EHR? This is really sort of a question that says even separating out all of this interesting discussion about information exchange, should there be certification criteria around this whole issue of corrections to make sure that EHR has the capability to do this? I think one of the things that was driving this question was some feedback that corrections were either couldn't be done or difficult to do in some EHR systems that have been certified. So that's one question.

The second question—it's actually the first question that's on the screen—starts to get into the information exchange is if a provider makes a correction to their EHR data and informs an HIO or other intermediary, does the HIO or other intermediary have any obligations to further propagate that information? In other words, does the HIO have to do something when they find out that there's a correction that's occurred?

So those are two questions and here on this screen is another series of questions, really respect to data quality and integrity and accuracy issues. The first one says, "What are the obligations of the source institutions with respect to notifying downstream recipients of various and modifications that the source detects?" So this is the situation where it's not a patient complaint but sort of like the example that I tried to give where the record is viewed a month or two later and somebody realizes there was a mistake in the record. Well if you're the source institution, do you have an obligation to notify everybody else who may have seen that record that is outside your organizational walls?

Second is the flip side is what about the recipient organization? If you're a physician office and you issue a summary information to say a hospital or to an ED for a patient, and the hospital or the emergency department looks at that data and they find an error in that data. Do they have an obligation to go back to the source organization and notify them that there was an error in that data? Then the third one is sort of perhaps a repeat of the previous screen, which is what is the role HIOs should play in this entire process of propagating corrections and/or mediating disputes.

Let me pause there and say, what do we think about these questions. Are these the right questions? Do we want to change these questions, add or delete anything to these questions or correct the questions?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
With respect to the second ones, are there obligations of recipients to propagate these notices when they share the information?

Deven McGraw – Center for Democracy & Technology – Director
Oh, when a recipient essentially becomes a source.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Sending on information they receive from somebody else.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think there's another good question that maybe is—I apologize I'm going to veer slightly close to the weeds here, but we're not currently certifying anything to do with the ability to actually detect whether integrity has been maintained since the creation of the document. We only certify on the transmission. It is certainly possible to certify with the digital signature that the document hasn't been altered anytime since it was originally created. I think it's a very valid question as whether certification should in fact require the ability to prove that the document hasn't been altered at all. That would of course apply to corrected versions, which would be resigned, if you would, so that you could still validate.

Paul Egerman – Software Entrepreneur
Yes. I'm trying to understand what you're suggesting David. Isn't that sort of like a different kind of correction that's to avoid a transmission error?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well it's an integrity check. We have integrity checks during the transmission process, but we don't have them anywhere else. We don't have them required anywhere else.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Except audit, which she had earlier.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Audit logs are required to be tamper proof but—so I can guarantee you that I send the document without corruption across the wire but the receiver could come in with a word processor and edit it and there's no way to tell that it's now a tampered-with document. Where this really matters is when the receiver is someone that you don't know you trust, for example possibly the patient through a PHR, and the patient says this document, this x-ray report which I had done last week on the other side of the country, here it is. And you provide it to the physician on this side of the country and there's no way to get it through an HIO, he doesn't have any way to trust that that document hasn't been tampered with but there's easy technology to solve that problem. It's actually part of the PCAST Report. It's a ... tracking and the digital signature. We … address that.

Paul Egerman – Software Entrepreneur
There's providence but you mentioned the PCAST Report. PCAST Report also suggest though that the recipient probably, or … probably, but frequently could alter the incoming information. The way that would occur would be if you sent information in SNOMED and I decided I want to receive it but I want it to translate into ICD-10, which is maybe that's what I need to do to get it to work in my system.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes and I think you've taken ownership of the data at that point, but if you wanted to validate that SNOMED code that was sent to you hasn't been tampered with, you don't have a way to do that today, other than through digital signatures, which is a well-established, well understood, standardized technology. That I'm not saying that we ought to impose it, but there would be distinct value to imposing that as a part of a downstream certification step particularly to the degree that it enables consumers to become trusted vectors of their own medical record, which in the long run, I think is the only way it's going to really work.

Paul Egerman – Software Entrepreneur
... this, so you're asking for—it's a different data integrity issue but your ….

Carl Dvorak – Epic Systems – EVP
Paul, I've got two comments. One is I think in a document centric world, you could make the argument that that's reasonable to do. Maybe even in a PHR world you could make the argument it's reasonable to do, but I think what happened is when these documents come in, they get expanded out and the data from those documents is used to update all sorts of information inside the receiving EHR. So although I agree with you that it's possible to do, I don't know it has as much practical benefit as people imagine it to have. Now if the document is temporarily held in someone else's hands while it's being transported. It

works for that case ... I will agree with that but I would be cautious in applying it to the general case of all HIE because I'm not as certain that it is generally applicable.

Then, back to your question on the other issue though of data being incorrect in the chart and the patient dealing with it, it is extraordinarily complicated to unwind those charts later because decisions are made based on other decisions based on other decisions that eventually trace a root back to misinformation in the chart. I think one of the patterns that we've seen with people dealing with this is they'll create a summarization entry and a way to stamp the chart as having had misinformation in it at one time. Then they'll summarize that misinformation and it's potential impact on the patient's care to date, and what one might be thoughtful about because it's not just the misinformation that matters now, it's all the other clinicians that might have taken real action on that patient but based on the misinformation. So we'll actually see in complicated cases, people make notes into the chart first off signaling that this has happened so that it's visible the next time a person comes to the chart, they'll be made aware of that this is one of those charts that's had somebody else's information comingled. Secondly, what if impact if any the new reader of the chart should be alert to as they process that information. So therefore, if we're going to pursue something down this path, they might want to think about, could we standardize a way in our vocabulary with which we communicate that something has happened to the chart just recognizing the complexity of how those interconnections are going to take place in the chart especially if it's had misinformation for some time.

Paul Egerman – Software Entrepreneur
Right, no that's a good comment. So is that a variation of this bottom question on the slide here about the technical capability of the EHRs? Are you saying that we … some standardize some terminology and ... or should we standardize terminology and capabilities for EHRs to handle these corrections?

Carl Dvorak – Epic Systems – EVP
I think for handling documentation that this record has previously had comingled data. What I worry about when you say standardized corrections, having lived in this for a long time, it's an abyss. It's not just hard. It's an abyss because of the complications that arise on dependent data and the interaction of human beings making decisions based on that data. The notion that you'll just correct it computer wise, it's not an EHR certification functionality. It might be a meaningful use, being able to comply with on audit or something, but I think from an EHR perspective, the critical thing is to be able to mark the chart, clearly signal to people that it's happened and have a human being's perspective on what the next person should be cautious about. We could certify things like removing unnecessary problems from the problem list, removing false allergies, removing meds the patient's not really on, but again once that med slips out into SureScripts world incorrectly, it'll still likely recycle back to you the next time you do a med update for that patient.

Paul Egerman – Software Entrepreneur
I think a lot interesting issues there, but again what we're trying to do right now is make sure that we simply understand what are the questions. So I wrote down in my notes, see if I've got this directly Carl, should we standardize how comingled data is handled or is … explained or is—

Carl Dvorak – Epic Systems – EVP
Should we create a standardized recommendation for signaling end users as to comingled data and the standardized method to document the potential impact of that and the method to share that information to downstream systems.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I would say these sound more like best practices to me than standards ... that weren't standard.

Carl Dvorak – Epic Systems – EVP
I agree with you. I think there's a practice element to it but if we're going to certify something that might be at that level of being able to send a package downstream to alert people as to what's happened because I think the technical correcting stream of data will confuse people downstream as much as it will help them.

Paul Egerman – Software Entrepreneur
At this stage right now, again we're just trying to understand what are the questions we want to answer. If we can answer it by saying, yes it's certification, we can answer it by saying, yes it's best practices. We can answer it by saying, well no.

Sue McAndrew – HITSP – Deputy Director
The general way to put that is how can we best protect patients against the downstream propagation of what were in fact genuine errors in their medical records.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I don't want to give up quite so easily on my notion that this content should be protected against the alterability, provably protected with a signature.

Paul Egerman – Software Entrepreneur
Isn't that a different issue though than what we're talking about?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's the integrity issue. It was three slides ago—four slides ago.

Deven McGraw – Center for Democracy & Technology – Director
It's an integrity issue. It's not one that we focused our set of questions on.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right, but I thought the whole set was what we were talking about or are we not supposed to comment on the integrity and quality question.

Paul Egerman – Software Entrepreneur
No we can comment on whatever we want.

Deven McGraw – Center for Democracy & Technology – Director
No, I think though David that I would frame the question in terms of whether we ought to have a policy for protecting against the ability to alter or modify data rather than—I think it's the job of standards to actually specify the methodology.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, I'm just using an example digital cert is one example but it is technically possible via a variety of mechanisms many of which are well understood and actually have been standardized for healthcare to detect alterations of a downstream document at any time, not just during transit. We could make that an expectation at some point for systems. Again, think that the long range view that the consumer becomes a vector of much of their own health information, this becomes a critical component to acceptance by providers. Otherwise, providers tell me to a person that they won't accept the data.

Paul Egerman – Software Entrepreneur
Well okay, so we'll write that down as a question. We … be debating the correct answer to that. If that's the question you want us to add to our list, we should add it to the list and then when we get to it we can do. Let me see if I wrote it down right though. What should it say, David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Should the data integrity protections offered by HIPAA to data in transit be expanded to include data—static data or the data after it's been delivered? I can think of better wordsmithing and send it to you.

Paul Egerman – Software Entrepreneur

If you could do that, that would be helpful.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's my notion is that HIPAA protects it during a brief window of its existence. The very technology that does that is capable of protecting it for broader slots of time.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What you're really talking about is protecting integrity for data at rest rather than in motion.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. It's for the life cycle of the data in a sense. It's non-repudiation. It's the standard stuff that—I mean the legal world does it, everybody does it except healthcare.

Carl Dvorak – Epic Systems – EVP
I'm not sure I totally agree with that David. I don't believe everyone does it, and I think it really applies well in a document centric world but it does not necessarily apply well if that data from a document is dispersed out through many, many other functions.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well Carl I agree that once the document is disassembled then the new person is taking ownership of that data and a new ... would apply, but if you consider a CCD or a CDA to be a document—

Carl Dvorak – Epic Systems – EVP
I do.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
—then I think that thing could have thousands of data elements in it and be shown to be untampered with from a source system.

Carl Dvorak – Epic Systems – EVP
Again, I agree with that but that's different than all data at rest. I just want to be careful with—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I agree.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We're really talking about once you've reconstructed the document—it's really a document, a document that is been exchanged and you want to check the integrity of that old document.

Paul Egerman – Software Entrepreneur
This is a good discussion but I'm afraid that we're going to answer the question, which we're really supposed to be asking the questions right now. So why don't we just ask you David to, since you're raising it, to draft the wording and then what we'll do is we'll put it on our list and we'll repeat this discussion.

Are there any other questions that should be addressed that we haven't addressed here relating to corrections?

Deven McGraw – Center for Democracy & Technology – Director
I wrote down Leslie's formulation of the overarching question, which I think is a good one for which there are probably a lot of little questions nested within it. How to best protect patients against the downstream propagation of an error in their health information, which gets to all of the sort of little questions that we have on slide 19 about what should the source do, what should the recipients do, both backwards and what's the backwards obligations as well as the forward obligations. Are they for any type of correction or is there some sort of threshold for data that might be relied on to the patient's detriment and the way that HIPAA sort of drew a line between what someone might call a minor correction versus a major correction

that could have consequences. Or whether we don't want to try to draw those lines and we want everything to go is maybe another question.

Paul Egerman – Software Entrepreneur
Those are good issues. One observation I would make is we think about this, is a lot of these corrections that … request, either patients request or the providers frequently surface—well all of them are not clinically significant. Some of them are, but a lot of them aren't. So, we often need to be careful of that, keep that in mind.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
It's an interesting thing because just like—I forget who, I think it was John who made a comment about patients … who don't want anybody to know that they were …. Lots of times, I've seen physicians who view how the record is documented as like an element of pride. They want to make sure people know that they did the right thing and they want to make sure it's written with correct English. So, they will want corrections made if it's not written out correctly. Which in one sense is great, but in another sense, it's not necessarily always have an impact on patient is my observation.

Any other issues here? Do we think we have a good list of questions?

Deven McGraw – Center for Democracy & Technology – Director
We have a big list of questions. … good one though.

Paul Egerman – Software Entrepreneur
What do we want to do, Deven? We've got a few minutes left. Do we want to say this is a successful meeting and go to public comment or do we want to dive into one of these?

Deven McGraw – Center for Democracy & Technology – Director
I think we should declare victory on the day. I mean, it does—because we arguably would have only about, maximum 10 minutes, and these are pretty meaty issues. So, notwithstanding that we only have one more call—two more calls, really—before the June Policy Committee meeting, we probably should, at least, give ourselves an opportunity to get the question list right and start maybe figuring out some draft straw recommendations between now and the next meeting. There's also the work of the small group on certificate authorities has to get going. So, we're asking a lot of people, so I don't really mind giving them a little time back.

Judy Sparrow – Office of the National Coordinator – Executive Director
That's great.

Paul Egerman – Software Entrepreneur
Sounds great.

M
Thanks a lot, a whole 10 minutes.

Paul Egerman – Software Entrepreneur
Well, let's find out what we've got for public comment because maybe the public comment will be 20 minutes long.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, if you could see if anybody wishes to make public comment. While we're waiting, I'll try to arrange a call, first call, for that small group.

Deven McGraw – Center for Democracy & Technology – Director

Thank you, Judy.

Paul Egerman – Software Entrepreneur
Yes, thank you very much, Judy.

M
Deven, you're going to circulate these topics, correct?

Deven McGraw – Center for Democracy & Technology – Director
Yes, the questions or the topics or both?

M
Both.

Deven McGraw – Center for Democracy & Technology – Director
Okay, yes, sure.

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thanks everybody.

Paul Egerman – Software Entrepreneur
Thank you. Great, as usual. Terrific call.

Public Comment Received During the Meeting

1. The discussions with this group does not need to occur off-line.

2. There are two elements of scope that may be considered...one is type of transmission, the other is the transmitter...in the weeds quickly.